



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Hn

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,005	04/12/2001	Douglas A. Hardy	GE04591	9509
7590	06/28/2005		EXAMINER	
Stanley A. Schlitter JENNER & BLOCK, LLC One IBM Plaza Chicago, IL 60611			SHIFERAW, ELENI A	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/833,005	HARDY ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 14 April 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-20 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 7/19/02, 4/14/05.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

Final Rejection

Response to Amendment

1. Applicant's arguments with respect to original claims 1-20, amendment filed April 14, 2005 have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

Response to Arguments

2. Applicant argues that:
- a. Ganesan does not teach or suggest using these private keys to encrypt or decrypt a message or an initial software product, and Ganesan does not teach or suggest splitting the session key into two components as claimed on claims 1 and 11 (page 4 lines 18-24).
 - b. Ganesan does not teach or suggest using a user's private encryption key to encrypt the session key, splitting the user's private encryption key into first and second portions, providing the encrypted session key and first and second key portions to the user, combining the first and second key options to yield the user's private key, and using the user's private key to decrypt the session key (page 4 lines 25-page 5 lines 4).
 - c. Dependent claims 2-10, and 12-20 are allowable based upon their dependency on allowable claims 1 and 11 (page 5 par. 2).

However, Examiner disagrees with applicant.

Regarding argument (a), the prior art of record Ganesan teaches dividing a private key into two portions and using these private keys to encrypt data/hash message (col. 3 lines 56-57, col. 4 lines 61-62 and col. 6 lines 47-54) or decrypt an encrypted data/session key (col. 4 lines 49-51, and col. 9 lines 11-17), and also central authority key (CA key portions) is divided in to first CA key portion and second central key portion (col. 3 lines 56-58, and col. 5 lines 22-29) and used for encrypting data/session keys (col. 3 lines 64- col. 4 lines 2).

Regarding argument (b), Ganesan teaches using a user's private encryption key to encrypt the data/hash message (col. 4 lines 61-62, and col. 6 lines 47-54), splitting the user's private encryption key into first and second portions (col. 3 lines 55-58, col. 4 lines 38-40, and col. 5 lines 22-28), providing the encrypted session key/video and first and second key portions to the user (col. 5 lines 1-10, col. 4 lines 2-4, and col. 3 lines 56-58), combining the first and second key options to yield the user's private key (col. 2 lines 56-59), and using the user's private key to decrypt the session key (col. 4 lines 49-51, and col. 9 lines 11-17).

Regarding argument (c), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) and (b), the dependent claims stand rejected.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts

that the system of the prior art, Ganesan does teach or suggest the subject matter as recited in independent claims 1 and 11. Dependent claims 2-10, and 12-20 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated July 23, 2005. Accordingly, rejections for claims 1-20 are respectfully maintained.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

4. Claims 1, 5, 11, and 15 are rejected under 35 U.S.C. 102(b) as being anticipated by Ganesan (U.S. Patent Number: 5,557,678).

As per claim 1, Ganesan teaches method for enabling encryption and decryption of an initial version of a software product comprising the steps of:

generating a first encryption key (Ganesan Fig. 2 No. 202);
encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (Ganesan Fig. 2 No. 220; encrypting the message (software product) with the first key);

generating a first key portion of said first encryption key (Ganesan Fig. 2 No. 202, and col. 2 lines 52-58; d.sub.i);

calculating a second key portion by utilizing said first key portion and said first encryption key to generate a said second key portion such that the combination of said first key portion and second key portion form said first encryption key (Ganesan Fig. 2 No. 202, and col. 2 lines 52-58; d=di*dj);

providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product (Ganesan Col. 2 lines 56-59, and col. 4 lines 47-49; message (software product) is encrypted (message encrypted using authority key that is portions of the key) and provided to the user);

combining said first key portion and said second key portion to provide said first encryption key in said hardware product (Ganesan Col. 2 lines 56-69; d=di*dj); and

utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product (Ganesan Col. 2 lines 56-69, col. 6 lines 1-19, and Fig. 2 No. 222; decrypting the message (software product) using the key (the first and the second portion of the key is the first encryption key)).

As per claim 11 a method for providing for the security of encryption keys for encryption and decryption of an initial version of a software product provided by a provider to a user of a hardware product, said method comprising:

providing a first encryption key (Ganesan Fig. 2 No. 202);

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (Ganesan Fig. 2 No. 222);

providing a first key portion (Ganesan Fig. 2 No. 202, and col. 2 lines 52-58; d.sub.i);

utilizing said first key portion and said first encryption key to calculate a second key portion such that the combination of said first and second key portions form said first encryption key (Ganesan Col. 2 lines 56-59, and col. 4 lines 47-49; message (software product) is encrypted (message encrypted using authority key that is portions of the key) and provided to the user);

storing said first key portion in storage means external to the hardware (Ganesan Col. 5 lines 29-34, and Col. 6 lines 21-31; storing the portions of the key on the device (hardware), and portions of the key can be stored separately);

storing said second key portion separately from said first key portion in a tamper proof memory means in the hardware product (Ganesan Col. 5 lines 29-34; storing the portion of the key in a secure area);

storing said encrypted software product in a further memory means in the hardware product (Ganesan Fig. 5 No. 504, and col. 10 lines 49-50; storing the encrypted data on the device (hardware));

combining said first key portion and said second key portion in the hardware product to provide said first encryption key (Ganesan Col. 2 lines 56-69; $d=d_i*d_j$); and

decrypting said encrypted initial software product with said first encryption key (Ganesan Col. 2 lines 56-69, col. 6 lines 1-19, and Fig. 2 No. 222; decrypting the message (software product) using the key (the first and the second portion of the key is the first encryption key)).

As per claim 5, Ganesan teaches the method further enabling an update of said first encryption key to provide a second encryption key to secure a different version of the initial software product, further comprising the steps of:

generating the second encryption key (Ganesan Fig. 2 No. 202; encryption key is generated it is obvious to generate the second encryption key because it would be different from the first encryption key and enhance security);

encrypting the different version of the initial software product with the second encryption key to provide an encrypted different version of the software product (Ganesan Fig. 2 No. 220; the message is encrypted using the encryption key it would be obvious to one ordinary skill in the art at the time of the invention was made to provide an encrypted different version of the software product with the second encryption key because it would be different from the first encryption key and enhance security);

combining the first encryption key and the second encryption key to provide a third key portion (col. 2 lines 57-59);

installing said third key portion and the encrypted different version of the software product in said hardware product (Ganesan Col. 5 lines 29-34, and Col. 6 lines 21-31);

combining said third key portion and said second key portion to generate a fourth key portion in said hardware product (Ganesan Col. 2 lines 56-69; $d=di*dj$);

combining the first key portion and the fourth key portion to provide said second encryption key in said hardware product (Ganesan Col. 2 lines 56-69; $d=di*dj$); and using the second encryption key to decrypt the encrypted different version of the software product (Ganesan Col. 2 lines 56-69, col. 6 lines 1-19, and Fig. 2 No. 222).

As per claim 15, Ganesan teaches the method further enabling security of an update of said first encryption key and providing a second encryption key for encrypting a different version of the initial software product, further comprising:

generating the second encryption key (Ganesan Fig. 2 No. 202; encryption key is generated it is obvious to generate the second encryption key because it would be different from the first encryption key and enhance security);

encrypting the different version of the initial software product with said second encryption key to provide an encrypted different version of the initial software product (Ganesan Fig. 2 No. 220; the message is encrypted using the encryption key it would be obvious to one ordinary skill in the art at the time of the invention was made to provide an encrypted different version of the software product with the second encryption key because it would be different from the first encryption key and enhance security);

combining said first encryption key and said second encryption key to provide a third key portion (col. 2 lines 57-59);

installing said third key portion in said tamper proof memory means (Ganesan Col. 5 lines 29-34; storing the portion of the key in a secure area);

installing said encrypted different version of the initial software product in said further memory means in the hardware product (Ganesan Col. 5 lines 29-34, and Col. 6 lines 21-31);

combining said third key portion and said second key portion to generate a fourth key portion in the hardware product (Ganesan Col. 2 lines 56-69; $d=di*dj$);

combining said first key portion and said fourth key portion to provide said second encryption key in the hardware product (Ganesan Col. 2 lines 56-69; $d=d_i \cdot d_j$); and using said second encryption key in the hardware product to decrypt the encrypted different version of the initial software product (Ganesan Col. 2 lines 56-69, col. 6 lines 1-19, and Fig. 2 No. 222; decrypting the message (software product) using the key (the first and the second portion of the key is the first encryption key)).

Claim Rejections - 35 USC § 103

5. Claims 2-4, 6-8, 12-14, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan (U.S. Patent Number: 5,557,678) in view of Patel (U.S Pub. No. 2002/0071558 A1).

As per claims 2, 6, 12, and 16, Ganesan teaches all the subject matter as described above.

Ganesan does not explicitly teach random number generator.

However Patel discloses the method wherein said step of generating a first (second) encryption key utilizes a random number generator to generate said first encryption key (Patel page 5 par. 0050).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Patel within the system of Ganesan because it would produce portions of the key in using exclusive-or.

As per claim 3, Ganesan and Patel teach all the subject matter as described above. In addition

Patel teaches the method wherein said step of calculating a second key portion utilizes an "exclusive or" logic operation to combine said first key portion and said first encryption key to calculate said second key portion (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

As per claim 7, Ganesan and Patel teach all the subject matter as described above. In addition Patel teaches wherein said step of combining the first encryption key and the second encryption key utilizes an "exclusive or" logic operation to combine said first encryption key and said second encryption key to generate said third key portion (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

As per claim 13, Ganesan and Patel teach all the subject matter as described above. In addition Patel teaches wherein said step of utilizing said first key portion and said first encryption key to calculate said second key portion utilizes an "exclusive or" logic operation (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

As per claim 17, Ganesan and Patel teach all the subject matter as described above. In addition Patel teaches wherein said step of combining said first encryption key and said second encryption key to generate a third key portion utilizes an "exclusive or" logic operation (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

As per claim 4, Ganesan and Patel teach all the subject matter as described above. In addition Patel teaches Ganesan teaches the method wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation to combine said first key portion and said second key portion to provide said first encryption key (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

As per claim 8, Ganesan and Patel teach all the subject matter as described above. In addition Patel teaches wherein said step of providing said second encryption key utilizes an "exclusive or" logic operation to combine said first key portion and said fourth key portion to provide said second encryption key (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

As per claim 14, Ganesan and Patel teach all the subject matter as described above. In addition Patel teaches wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation performed by said hardware product (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

As per claim 18, Ganesan and Patel teach all the subject matter as described above. In addition Patel teaches wherein said step of combining said first key portion and the fourth key portion to provide said second encryption key utilizes an "exclusive or" logic operation (Patel page 3 par. 0022). The rational for combining are the same as claim 2 above.

Claims 9-10 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan (U.S. Patent Number: 5,557,678) in view of Ganesan (Ganesan '276, Patent No. 5,535,276).

As per claims 10 and 20, Ganesan teach all the subject matter as described above.

Ganesan does not explicitly teach non-sequential encryption key.

Ganesan '276 discloses non-sequential encryption key to plurality of users (col. 8 lines 9-19) in using split key ($d=di*dj$) (col. 2 lines 59-62) that reads on the method wherein said second encryption key is non-sequential with said first encryption key.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Ganesan '276 within the system of Ganesan because it would generate different encryption keys that are non sequenced. Therefore it would be obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings Ganesan '276 within the system of Ganesan because it would generate different encryption keys that are non sequential for different versions of software to enhance security.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/833,005
Art Unit: 2136

Page 14

Elen Shiferaw

June 23, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100